

Abstract of the Disclosure

The method of the invention assumes there is a security manager and mechanism present for defining, attaching, and evaluating external authorization policy to file resources based on the file's path name. In this invention, protected symbolic links and the resources that the link points to are stored in a protected object database. When a system access attempt occurs, the file attribute is extracted from the file used in the access. The file attribute is then used to search the protected object database. If a matching system resource is found, and that resource is protected but does not have independent security policy on it, then the resource will have the security policy of a symbolic link that points to it. In this case, the security of each protected symbolic link pointing to the system resource has to grant access in order for allowance of the access attempt. This approach insures that the most restrictive outcome prevails.